530-ARCH-NSM-NCCDS/1998

MISSION OPERATIONS AND DATA SYSTEMS DIRECTORATE

Network Control Center Data System (NCCDS) Network and Systems Management (NSM) Architecture

Volume 1
Revision 1

May, 1996

National Aeronautics and
Space Administration

Goddard Space Flight Center
Greenbelt, Maryland

Network Control Center Data System (NCCDS) Network and Systems Management (NSM) Architecture

Volume 1
Revision 1

May, 1996

Prepared Under Contract NAS5-31000
Task Assignment 369-8077

Approved By:

Roger Clason, Technical Representative Date
NASA GSFC Networks Division

Branch Management Approval:

Anthony Maione, NCC Project Manager Date
NASA GSFC Networks Division

Goddard Space Flight Center
Greenbelt, Maryland

Preface

This document defines a comprehensive Network and Systems Management (NSM) architecture for the Network Control Center (NCC) Data Systems (NCCDS) 1998 (NCC98) endeavor.

Questions and proposed changes concerning this document shall be addressed to:

Anthony Maione, NCC Project Manager
Code 530.5
Goddard Space Flight Center
Greenbelt, Maryland 20771

Abstract

This document defines and establishes a comprehensive architecture and components required for the Network and Systems Management (NSM) subsystem of the Network Control Center (NCC) Data System (NCCDS), 1998 (NCC98). The purpose of the NSM subsystem is to monitor and proactively manage the critical systems and processes of the NCCDS network, notify NCC personnel of critical network and systems events, generate network and systems activity summary reports, and utilize NSM tools for daily operations and troubleshooting tasks.

The NSM architecture consists of a centralized management platform based on industry-accepted standards to provide interoperability and compatibility among components. It integrates Commercial Off-The-Shelf (COTS) software packages to meet specific NCC98 goals and provide comprehensive monitoring and management of NCC98 systems. The NCC98 systems to be managed are:

- Service Planning Segment Replacement (SPSR)
- Network Protocol Gateway (NPG)
- Firewall
- Communications and Control Segment (CCS)
- LAN devices (hubs).

This document specifies the overall design goals and explains the methodology used to establish this architecture. It presents a high-level overview of the NSM architecture, followed by a detailed description of the required components and how they are integrated to form a comprehensive NSM system. Finally, the costs for each component are detailed, and the interfaces required between the NSM and other NCCDS subsystems are specified. A set of Functional Requirements satisfied by the NSM architecture, established from both the *NCCDS System Requirements Document (SRD), 1998 (NCCDS SRD 1998)* as well as interviews with Code 530.5 personnel, is presented in Appendix A.

Keywords: *network and systems management, NSM, architecture, monitoring, statistics, event notification, resource activity, troubleshooting.*

Contents

Preface

Abstract

Change Information Page

Change Information Page

DCN Control Sheet

1. Introduction

2. Architecture

3. Costs

4. Interface with NCC 98 Subsystems

Figures

Tables

1. Introduction

1.1 Purpose

This document defines and establishes a comprehensive architecture and components required for the Network and Systems Management (NSM) subsystem of the Network Control Center (NCC) Data System (NCCDS) 1998 (NCC98). The purpose of the NSM subsystem is to monitor and proactively manage the critical systems and processes of the NCCDS network, notify NCC personnel of critical network and systems events, generate network and systems activity summary reports, and utilize NSM tools for daily operations and troubleshooting tasks.

This document specifies the overall design goals and explains the methodology used to establish this architecture. It presents a high-level overview of the NSM architecture, followed by a detailed description of the required components and how they are integrated to form a comprehensive NSM system. Finally, the costs for each component are detailed, and the interfaces required between the NSM and other NCCDS subsystems are specified. A set of Functional Requirements satisfied by the NSM architecture, established from both the *NCCDS System Requirements Document (SRD), 1998 (NCCDS SRD 1998)* as well as interviews with Code 530.5 personnel, is presented in Appendix A.

1.2 NCC98 Background

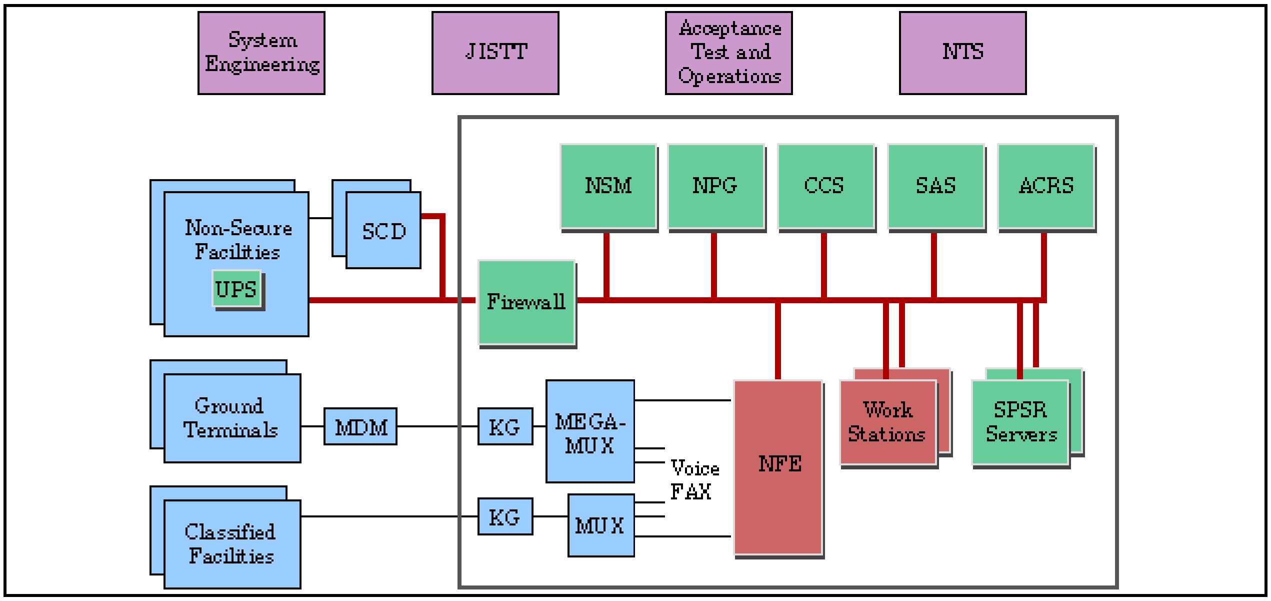
The NCC is an element of the National Aeronautics and Space Administration (NASA) Spaceflight Tracking and Data Network (STDN). It is responsible for network resource scheduling, acquisition support, data quality assurance, performance monitoring, and overall coordination of the STDN and must be operational twenty-four (24) hours a day, seven (7) days a week. To complete its mission, the NCC utilizes the five major segments of the NCCDS: Communications and Control Segment (CCS), Service Planning Segment Replacement (SPSR), Automatic Conflict Resolution System (ACRS) Tracking and Data Relay Satellite (TDRS) Look Angle System (TLAS) (ACRS/TLAS), Service Accounting Segment (SAS), and System Resources and Infrastructure Segment (SRIS).

Currently, existing NCCDS systems use a proprietary networking protocol, the NASA Communications (NASCOM) 4800 bit-block (BB) protocol, custom switches and network control software, and in-house software applications operating on legacy systems. Such a non-standard environment is expensive to maintain and creates interoperability issues when attempting to connect to external networks that comply with Open Systems Interconnect (OSI) standards. NCC98 is an effort to redesign these subsystems and infrastructure, conforming to OSI standards wherever possible.

The current design for the NCC98 network specifies four isolated Local Area Network (LAN) segments to be used for Operations, Development, Test and Training, and Integration Testing. These LAN segments will be interconnected via commercially available switching hubs that satisfy the de facto network management protocol standard, the Simple Network Management

Protocol (SNMP). The NCC98 LANs will use the Transmission Control Protocol/Internet Protocol (TCP/IP) standard networking protocol among NCCDS subsystems. External NASCOM systems that use the NASCOM 4800 BB protocol will connect to the NCC through a Firewall and pass through the Network Protocol Gateway (NPG) subsystem, where a protocol conversion to TCP/IP will occur. Figure 1-1 shows the proposed NCC98 design, as specified in the *NCCDS SRD 1998*.

Figure 1-1: High-Level NCC98 Architecture (Proposed)



The NSM subsystem is part of the SRIS component and will be implemented as part of NCC98 to provide an automated means for monitoring and proactively managing relevant NCCDS systems and LANs. The major NCC98 components that will be managed by the NSM are as follows: SPSR, NPG, Firewall, network connectivity devices (i.e., hubs), and, to a limited extent, CCS. The ACRS/TLAS subsystem will not be managed by the NSM. With the exception of CCS, these managed systems will be hosted on UNIX-based platforms including an HP K210 server and several HP C-class workstations. CCS will continue to reside on a VAX 8550 for the foreseeable future.

1.3 NSM Goals and Methodology

The broad goal of the NSM is to prevent network and system faults from adversely affecting NCC operations while maintaining the highest level of services to users. More specifically, however, the NSM must meet a particular set of requirements that have been defined in the *NCCDS SRD 1998*. These requirements may be generalized to include the following goals:

- Centrally monitor and manage network and system resources on the following systems: SPSR, NPG, Firewall, SNMP-manageable devices (e.g., hubs, switches, servers, workstations), and CCS;
- Notify NCC personnel of critical network and systems events that would impact NCC operations;
- Monitor utilization of network and systems resources through real-time data collection and historical trend analysis;
- Generate resource activity summary reports for capacity planning and to verify RMA requirements;
- Maintain startup and shutdown configurations for SPSR, NPG, and Firewall;
- Provide the capability to modify existing SPSR, NPG, and Firewall configurations and coordinate automatic failover to backup systems; and
- Provide an audit trail for security and accounting purposes.

To gain a better understanding of NCC98 requirements, specific NCC98 design and operations personnel were interviewed extensively. The responses from the interviews and the Functional Requirements specified in the *NCCDS SRD 1998,* were consolidated into a Functional Requirement Validation table that is provided in *Appendix A* of this document. The proposed NSM architecture conforms to these validated functional requirements.

NOTE

> The Functional Requirements Validation presented in *Appendix A* is not intended to be a formal Functional Requirements document. The requirements specified in *Appendix A* are refined versions of the formal Functional Requirements and are intended only to assist the NSM team in designing the NSM.

To provide a point of departure for the design of a comprehensive NSM system, the validated Functional Requirements were partitioned into the five standard OSI network and systems management areas. These OSI functional network and systems management areas are described in the next section. The proposed NSM architecture was based on a combination of the validated Functional Requirements and analysis of the task according to the OSI NSM areas.

The proposed NSM Architecture has been based on existing standards, particularly SNMP. It relies minimally on custom-created tools and integrates Commercial-Off-The-Shelf (COTS) products into an integrated NSM framework. This philosophy is intended to ensure scaleability to support expansion and the addition of new technology as it becomes available. Additionally, it is designed to be user-friendly and empower non-technical personnel to obtain and act on available network and systems resources. Finally, the NSM is designed to impact as little as possible on available network and systems resources.

1.4 OSI Network and Systems Management Functional Areas

OSI defines five standard network and systems management functional areas: Accounting Management, Configuration Management, Fault Management, Performance Management, and Security Management. A sixth, non-standard functional area, General Systems Management, has been added for the purposes of this architecture to describe the infrastructure necessary to support the NSM. This section provides a brief description of these functional areas.

1.4.1 Accounting Management

Accounting Management provides the ability to track usage of NCC98 resources, log critical information for later review, and provide an audit trail to track resource usage. This includes, but is not limited to, the following:

- Suspicious network activity;
- System generated reports; and
- Usage logs.

1.4.2 Configuration Management

Configuration Management provides the ability to manage NCC98 assets and enforce system-wide network and systems standards. These functions include, but are not limited to, the following:

- View and configure/reconfigure intelligent devices on the network;
- Initialize and shut down network elements; and
- Collect and maintain information about the condition of a network component in an inventory control database.

1.4.3 Fault Management

Fault Management is the process of detecting, isolating, and correcting abnormal network and systems operations. A fault results from the failure or degradation of a system, application, process, circuit, or device. Fault Management responsibilities include:

- Monitor and correlate alarms;
- Maintain Reliability-Maintainability-Availability (RMA) levels;
- Verify connectivity;

- Detect and isolate problems; and
- Suggest resolution options.

1.4.4 Performance Management

Performance Management provides NCC98 personnel with the ability to measure, analyze, and predict the behavior of network and systems resources. This includes such metrics as:

- I/O activity;
- CPU and disk utilization;
- Database transaction processing time;
- Bandwidth utilization data;
- Ethernet frame collisions; and
- Packet errors.

These metrics can assist in planning to increase capacity or to integrate new technology.

1.4.5 Security Management

Security Management provides the ability to safeguard proprietary data and ensure system integrity against unauthorized access. Specifically, Security Management is a compilation of network controls and monitoring mechanisms that enforce accountability, assure data integrity, control access, prevent accidental or malicious disclosure, and assure network availability.

1.4.6 General Systems Management

To achieve an adequate level of NSM conformance, a number of preliminary requirements must be met. These requirements are general in nature but are necessary to meet one or more needs of the OSI functional areas. General Systems Management requirements concern issues such as SNMP configuration, customization, user account management, and backup and restore.

2. Architecture

2.1 High-Level Architecture Design

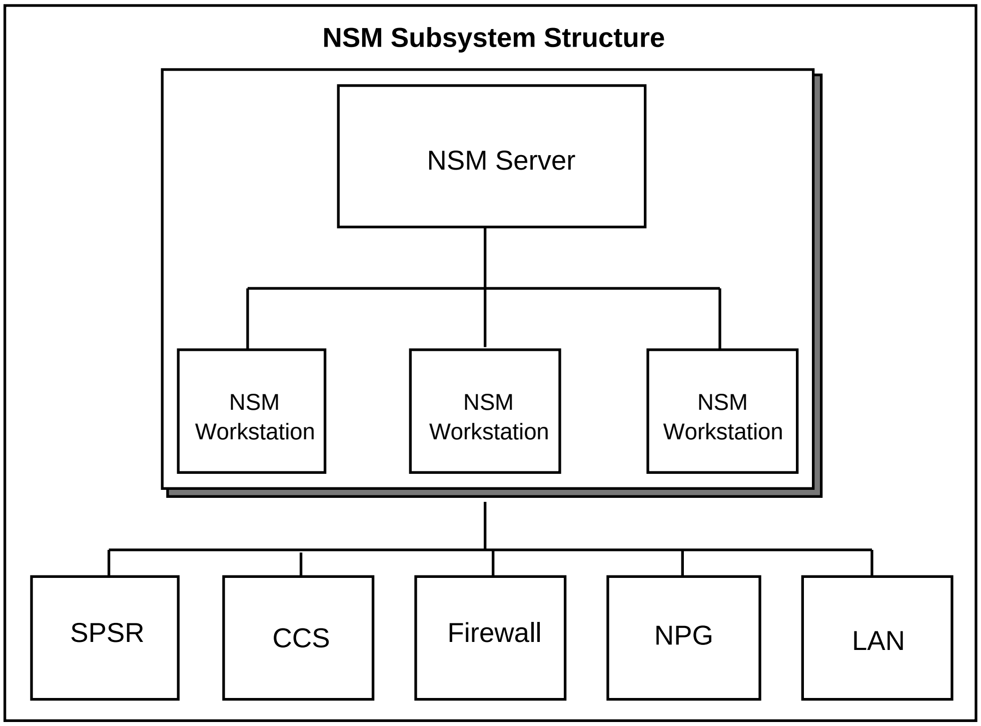
The proposed NSM architecture is based on a central management platform that will provide monitoring and proactive management for the NCCDS systems, notification to NCC personnel of critical network and systems events, generation of network and systems activity summary reports, and utilization of NSM tools for daily operations and troubleshooting tasks. It is based on COTS tools which conform to existing management standards, that can be expanded or exchanged to meet the dynamic needs of the NCC. The management platform itself is modular and consists only of integrated hardware and software components. As new technology and requirements are introduced, tools that are compliant with the NSM management platform can be easily implemented, integrated, and transitioned into operations.

The NSM management platform is comprised of a single server located within the NCC. The server will house the integrated COTS tools that comprise the NSM solution and perform all of the processing necessary to maintain the NSM. Additionally, the server will contain an NSM database that will store network and systems resource data, trouble tickets, and configuration information. Multiple-operator access to the NSM will be provided through client workstations at points within the NCC.

The NSM workstations will have the ability to display status information and statistics from any of the NCC LANs. Each LAN will represent a specific management domain that can be accessed either manually or by default, depending on NCC operator login or group. The workstations can be configured to display either isolated views of different aspects of the NCCDS systems and LANs, according to NCC operator login or group, or a view of the entire NCC network.

Figure 2-1 presents a generic view of the proposed management platform. The NSM subsystem will be logically connected to the OpsLAN components of SPSR, CCS, Firewall, NPG, and the LAN architecture. The subsystem will be comprised of the NSM server and its associated workstations.

Figure 2-1: Management Platform and Servers



2.1.1 Selected NSM Applications

The NSM management platform will be based on the following tools:

- **HP IT/Operations (IT/O)**—the framework for integration for all NSM applications. This product acts as an SNMP element manager to perform status polling, notifications, and display of network topology. Configuration into distinct managed domains is also included to partition management responsibilities to each responsible party;

- **Remedy Action Request System (ARS)**—a third-party application to generate trouble tickets, provide notifications, and track events;

- **HP NetMetrix**—an integrated software application that collects resource utilization statistics from SNMP and RMON-compliant devices and provides trend analysis and report generation capabilities;

- **HP Omniback II**—a third-party application to provide system-wide backup;

- **BGS BEST/1**—a third-party application to provide process monitoring and statistics for the NCCDS subsystems, forwarding event notifications to the element manager;

- **Oracle**—a relational database management system (RDBMS) for storing information from the management platform;

- **Spider**—a WWW-to-database interface that provides simple development of WWW-browser based SQL queries; and

- **Netscape**---a WWW server and browser for providing information from the management platform to users.

Each tool has been recommended due to its ability to meet the NCC98 network and systems management requirements as defined in *Appendix A.* Table 2-1 shows each tool that will be deployed on specific NCCDS systems. Related software components, e.g., IT/O Server, Client, and Agent, are on the same row.

Table 2-1: NSM Tool Deployment

	Subsystem						
Tool	**NSM Server**	**NSM Workstations**	**SPSR**	**NPG**	**Firewall**	**CCS**	**LAN (hubs)**
HP IT/O Server	X						
HP IT/O Client		X					
HP IT/O Agent	X	X	X	X	X	X	X
HP NetMetrix Server	X						
Remedy ARS Server	X						
Remedy ARS Client	X	X					
HP Omniback II Server	X						
HP Omniback II Client	X	X	X	X	X		
BEST/1-Monitor	X	X					
BEST/1 Visualizer	X	X					
BEST/1 Predict	X	X					
BEST/1-Agent	X	X	X	X	X	X	
Oracle7	X						
Spider	X	X					
Netscape Server	X						
Netscape Client	X	X					

NOTE

> The table above lists *only* the NSM tools that are deployed on each subsystem. It does not attempt to address software that may already exist on specific subsystems due to other subsystem requirements.

To ensure optimum integration of applications, each tool must meet certain criteria regarding operating systems, hardware compatibility, compatibility with the integration framework, and compliance with standards. Specifically, each tool must be compatible with the HP-UX 10.x operating system, be compliant with the HP OpenView (OV) network management suite, support Oracle7 as its relational database engine, and be able to operate on an HP J-class workstation running a PA-RISC 7200 HP chip. Table 2-2 lists compatibility issues for the selected tools. An X in a column indicates compatibility with that column; an O indicates it is not compatible. An N/A entry indicates that it is not applicable to this tool.

Table 2-2: NSM Tool Compatibility Matrix

Product	HP-UX 10	Oracle 7	HP J/C	HP OV
HP IT/Operations	X	X	X	N/A
Remedy ARS	X	X	X	X
BGS BEST/1 Performance	X	X	X	X
HP NetMetrix	X	X	X	X
Oracle 7	X	N/A	X	N/A
Spider Technologies Spider	X	X	X	O
Netscape Server and Netscape Navigator	X	N/A	X	N/A

2.1.2 NSM Functionality Overview

At its most basic level, the NSM will monitor and manage specific NCC devices. The subsystems to be monitored are:

- SPSR;
- NPG;
- CCS;
- Firewall; and
- LAN devices (hubs).

This section will provide an overview of the functionality that the NSM will deliver.

Figure 2-2 presents a high-level overview of how the NSM components integrate to provide a comprehensive network and systems management solution for NCC98.

Figure 2-2: NSM Integration

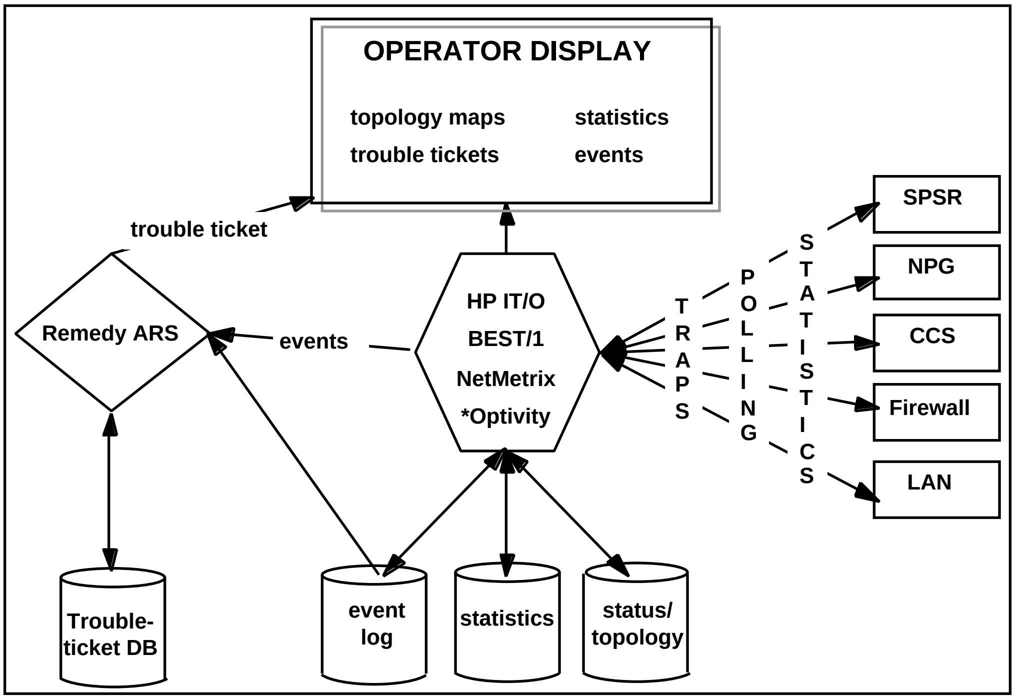


Figure 2-2 presents a high-level diagram of the functionality of the NSM, how the NSM relates to the systems it manages, where NSM information is stored, and what an NCC operator will see on the console. As is shown, four major components will integrate at the NSM server to monitor the managed subsystems. These four components will perform status polling, gather statistics, and receive traps from the NCCDS subsystems.

Separate databases will be updated from the NSM server, including an event log, a statistics database, and a status and topology map database. A separate component of the NSM, the Remedy ARS trouble-ticketing system, will receive notification of events from the NSM base component. Upon receipt of an event, the trouble-ticket component will update a fourth database to store trouble-ticket information and send notification of events to the NCC operator at the NSM workstations.

At the NSM workstations, the NCC Operator will have the ability to monitor topology and status maps, display resource utilization statistics, receive and update trouble tickets, and view subsystem configuration information. Using a standard HyperText Markup Language (HTML) browser, the NCC Operator will have the ability to modify and update configuration information. The integration of the various components that comprise the NSM is explained in greater detail in the next section.

2.1.3 Detailed NSM Functionality

The NSM server will perform status polling on all devices in its domain that use the IP protocol. This includes all servers, workstations, and hubs that are connected to the NCC LANs. The NSM server will display the configuration of the network topology in the form of maps and submaps that show device status according to color. NSM workstations will have access to this information through resident client software.

The NSM server can receive information on network and systems events from agent software that resides on the managed nodes. A network or systems event is an abnormal condition that occurs on a managed device. Events can be generated in a variety of ways. The NSM server can initiate an event if a device fails to respond to a status poll. The agent software on the managed nodes can forward an event to the NSM server if it detects that a critical process has failed or if a pre-determined threshold has been exceeded by the system. The Simple Network Management Protocol (SNMP) compliant managed nodes can also forward an SNMP trap for specific conditions. Finally, the performance monitoring software can generate an event if network utilization thresholds are met.

When a critical network or systems event is detected, the NSM server will either generate a trouble ticket or initiate corrective action. Corrective action will be initiated only in specific instances that have been predefined by the NSM administrator. In the case of a generated trouble ticket, the appropriate NCC personnel will be notified. These notifications can be sent to both individuals and/or groups, or escalated to supervisory personnel. The trouble ticket can be displayed at the NSM workstations, sent via electronic mail, transmitted to a paging device, or signaled through an audio device.

The NSM will provide automated and manual failover capabilities for three subsystems: SPSR, NPG, and the Firewall. To provide this functionality, configurable agent software will reside on each of these subsystem servers. A configurable agent is a software tool that runs in the background on a particular system. It can be customized to monitor specific processes and resources. In the event that any of the critical processes performs erratically, the agent will perform one or a combination of several tasks: 1) provide notification to the NCC Operators via an SNMP trap, 2) attempt to restart the erratic process, or 3) launch a failover process. The action that is performed will depend on the set of conditions surrounding the erratic performance.

The NSM has also been designed to monitor NCCDS resource utilization statistics which can be stored in and retrieved from the NSM database for later analysis. From an NSM workstation, the NCC operator will be able to display both real-time utilization data and historical data. A few examples of statistics that the NCC operator will be able to examine include:

- Bandwidth Utilization, broken out by protocol;
- TopN Conversation partners on a LAN;
- Number of octets transmitted;
- CPU utilization according to time;

- Number of database transactions; and
- Collisions according to time.

Additionally, the NSM server can be configured to automatically generate resource utilization reports for trend-analysis and capacity planning purposes.

Subsystem configuration information will reside in the NSM database. The NCC operator will be able to update this information through a Structured Query Language (SQL) Query Form displayed on a Netscape Navigator browser. When the configuration information is updated and a commit-transaction instruction is signaled to the NSM database, the NSM server will perform the following actions:

1. Fail over the primary subsystem to its backup.
2. Stop the primary subsystem process.
3. Update the configuration of the primary subsystem.
4. Restart the primary subsystem in the new configuration .
5. Fail over the backup subsystem to its primary .
6. Update and restart the backup subsystem.

This will provide timely and simplified configuration management for the NCC.

2.2 Detailed Architecture Components

2.2.1 Hardware Components

In order to provide the best support to the NCC98, a robust and reliable system must be utilized. The NSM server will have to provide, at a minimum, the following capabilities:

- Dual processors
- Tape drive
- CDROM
- 8 Gigabyte (GB) Disk Space
- 512 Megabyte (MB) Memory.

The Hewlett Packard 9000 J-Class Workstation Model J210 provides the necessary functionality to support the NCC98 NSM enterprise as the central server. This workstation provides dual 120 Megahertz (MHz) PA-RISC 7200 processors. With dual processors, the J210 can dedicate one processor to running the NSM applications and reserve the second to handle all database transaction processing. The J210 comes equipped with sixteen (16) Single, In-Line Memory

Module (SIMM) slots. The current NSM task will require eight of these slots, providing 512 MB of memory. The remaining eight slots may be used for expansion at a later time.

The J-Class workstation accommodates a maximum of two internal disk drives, which provides ample storage space for both NSM applications and database storage of historical network and systems resource data. The NSM will utilize both drive bays. The first slot, holding a 4 GB disk drive, will store the NSM operating system and software tools, and the second, with a 2 GB disk drive, will store the databases needed by the NSM. Additionally, the J210 workstation supplies two internal removable media drives which meet the needs of the NSM. The first will be filled with a 4 GB Digital Data Storage 2 (DDS2) Digital Audio Tape (DAT) tape drive which can be expanded to 8 GB of storage with typical compression. The second will house a quad-speed CD-ROM drive to be used for software installation and upgrades. Finally, the J-Class workstatation provides a 20" color graphics monitor with standard keyboard and mouse.

The NSM also requires the use of three (3) workstations which will serve as NSM client consoles. The client consoles will reduce X-related traffic on the NCC LANs to optimize LAN utilization. These consoles will be located in the NCC for use by NCC operations staff. The HP C-Class Workstation Model C100 with a single 100 MHz PA-RISC 7200 processor will be used to fulfill this need. This workstation model is consistent with current requirements for other subsystem workstations in the NCC and has been chosen due to its future upgrade capability. The workstation supports eight (8) SIMM slots, 2 of which will be utilized for the current NSM task, providing 128 MB of memory, with the other six (6) available for expansion at a later time. This workstation also supplies one internal removable media drive which will be used for a CD-ROM and two internal disk drive slots. The NSM clients will use one slot for a 2 GB disk drive. The additional slot will be free for expansion at a later time. Finally, the Model C110 provides a 20" color graphics monitor with standard keyboard and mouse, necessary for viewing the status of the entire NCCDS network.

All four workstations, both J-class and C-class, will run the most current stable version of the HP-UX Operating System and come packaged with two Run-Time user licenses and the necessary vendor documentation. The J-Class workstation, due to an HP IT/O licensing requirement, will require an additional eight user license to be installed.

2.2.2 Software Components

This section describes in detail the selected COTS products that will be integrated to form a comprehensive NSM solution for NCC98.

2.2.2.1 HP IT/Operations Center

The core component of the NSM solution is HP OpenView IT/Operations Center (IT/O). IT/O integrates two proven performers in the network and systems management arena into a comprehensive NSM solution: HP OpenView Network Node Manager (NNM) and HP OpenView Operations Center (OpC).

IT/O is a distributed client/server software solution in which the server acts as a central management console, and the clients access the server database without generating X-traffic across the LAN. IT/O intelligent software agents reside on the managed nodes and provide information on system resources, security, and status. Full control of distributed Information Technology (IT) resources across the enterprise is available from the central management system, enabling the identification and resolution of potential problems before end-users are affected. The intelligent agents can also be configured to solve problems without interacting with the central management system.

IT/O has the ability to collect information from distributed multi-vendor computing environments, process the information, and determine and report the status of elements within the environment. IT/O can graphically show the current status of all of managed elements within the NCC enterprise including networks, systems, applications, and databases. The status information is presented to NCC operators using color-specific icons and detailed view maps. All managed elements are handled in a consistent and technology-independent way, thereby providing what appears to be a single homogeneous managed environment. All of the collected information and activity logs are stored in a central data repository that can provide historical data and trend analysis.

IT/O offers the ability to define SNMP thresholds and monitor intervals and receive network, systems, database, and application messages and events. Once a threshold value is exceeded, IT/O intelligent agents can run a pre-defined automatic action and/or generate and send a message to alert an NCC operator at an NSM client console. Messages and events can also be forwarded to a pager or trouble-ticketing application.

To help focus on the most critical problems, the IT/O Message Browser Window sorts incoming problems and events into six severity levels, from stable to critical-state. These severity levels can be displayed according to priority to assist the NCC Operator in prioritizing problem resolutions and event responses. IT/O events are stored in a historical database that allows the overall health of the NCC enterprise to be audited and analyzed. This database can assist NCC personnel to identify trends and anticipate problems before they occur.

The IT/O display can be customized to clearly define NCC operator roles and individual management domains. The NCC operator roles can be defined according to area of expertise or subsystem to be managed, and the associated display can be customized to show either the particular subsystem or the entire NCC enterprise. Network and systems activity displays and reports can also be customized to meet the operators needs.

In addition to these features, IT/O provides multiple mechanisms for handling critical conditions. These mechanisms are comprised of automatic or manual actions, problem-specific help texts and instructions, and operator notification. In specific instances , the intelligent agents can also initiate and execute corrective actions without any involvement from the NSM server.

Other specific functionality of IT/O includes:

- Monitors CPU and disk utilization through customizable IT/O intelligent agents;
- Provides continuous data collection on system resources;
- Provides a graphical display of network and system faults;

- Allows view of actual message details and system performance graphs;
- Integrates with HP Omniback II to provide network-wide comprehensive tape management and backup; and
- Indicates failed login attempts and unauthorized access incidents through security reports.

IT/O was chosen as an integration framework on the basis of both its above functionality and its wide acceptance in the industry. This acceptance is illustrated by the following features:

- The HP OpenView suite of products has open, well-published application programming interfaces (APIs) which significantly reduce the need for custom software development.
- IT/O meets OSI network standards, including the de facto management standard protocol, SNMP, thereby ensuring compatibility with other compliant applications and products.
- The HP OpenView suite of products has captured the largest market share of the network and systems management platform market. As a consequence, a large number of third-party applications have been developed to integrate with and enhance network management functionality provided by OpenView.
- Management platform competitive technology, such as IBM NetView and Digital, are based on HP OpenView core technology.
- The HP OpenView suite has the best record of maintaining backwards compatibility that provides investment protection against obsolescence.

IT/O serves as an integration point for a wide array of third-party products that provide more specific or vendor-specific functionality. As such, IT/O will provide a robust, scaleable framework for the NSM subsystem, compliant with OSI standards, to meet specific NCC98 goals.

2.2.2.2 Remedy ARS

The NSM has the requirement to notify an NCC operator in the event of a network or system warning, error, or failure. Notification can take the form of an electronic message, graphical display, or paged signal. Notifications follow a specific sequence of generation, assignment, tracking, modification, and resolution. The primary mechanism in providing this functionality is the automated trouble ticket system. The trouble ticket tool recommended to the NCC98 NSM is Remedy ARS.

ARS is a powerful, flexible, and scaleable system that can automate process flow and event resolution to meet NCC98 needs. ARS integrates with IT/O to identify network problems, record information, and route the current problem to the appropriate support personnel. ARS is based on an easy-to-use Graphical User Interface (GUI) that uses an Oracle database. Trouble ticket templates are also available and are customizable to support specific network and systems needs.

The Remedy ARS system will be located on the NSM server. The NSM workstations will host an ARS client and an Oracle interactive user license. The server and ARS clients will be located in the NCC. The following components are required to implement the ARS architecture:

- ARS Server (1)
- ARS Clients (4)
- Oracle interactive user licenses (4).

ARS provides two different types of trouble ticket generation. These specific functions of ARS are discussed in the next two sections.

2.2.2.2.1 Automatic Trouble Ticket Generation

When an event occurs on a managed network device or system, a trap is sent to IT/O. This trap contains specific information on the device that generated an error and necessary information describing the error that occurred. Upon receipt of the trap, IT/O changes the status and color of the device icon on the graphical display to account for the error. The ARS system takes this information and automatically opens a trouble ticket, auto-populating certain fields from IT/O. Once these fields are populated, the trouble ticket is forwarded to the predetermined NCC support personnel. The NCC support personnel are notified via graphical display, E-mail, or pager. Graphical displays and E-mails are the standard form of notification. However, if the error is a high priority, paging notification will be used.

In addition to the above capabilities, ARS incorporates rules for escalating a trouble ticket to the next level of support if it is not attended to within a pre-set amount of time. Once a problem has been resolved, IT/O recognizes the device as operational, and ARS closes the trouble ticket.

2.2.2.2.2 Manually Generated Trouble Tickets

ARS provides all of the functionality that is required for standard operational activities of a network control center. When a call is received by the NCC operator, a trouble ticket can be opened manually using the ARS client to enter the necessary information into a “problem entry” screen. Some fields on this screen will have an active link to schemas which will automatically populate related information from IT/O. From this screen, the NCC operator can add a new caller to the trouble ticket, list open, related, and duplicate tickets, and access a database of possible problem solutions. As each ticket is resolved, the information is transferred to the problem resolution database. This database can be accessed using a Case Based Reasoning (CBR) tool or queried via a full text search. If a ticket cannot be resolved interactively, it will be logged and then sent to the appropriate NCC support personnel. Notification and escalation procedures are the same as those for automated generation of a trouble ticket.

2.2.2.2.3 Trouble Ticket Schema

Based on previous experience from other network and system management systems, the following schema is provided. This schema is not to be taken as a final draft and is supplied only to provide a general understanding of the trouble ticket system. The table below describes generic schemas which may or may not be implemented into the NSM.

Table 2-3 indicates a field and the associated data source for that field. Each schema and field should be reviewed and evaluated by NCC personnel as to its usefulness to the network and systems operations only. The final schemas will be presented at implementation of the NSM.

Table 2-3 Trouble Ticket Schema

Schema	Source
Event Type Schema	**Data Source**
Event Id (key field)	IT/O
Event Name	IT/O
Event Description	IT/O
Recommended Test Procedures	ARS Database
Notification Mechanism	ARS Database
Priority	ARS Database
Vendor Schema	**Data Source**
Vendor (key field)	ARS Database
Vendor Phone	ARS Database
Vendor First Name	ARS Database
Vendor Last Name	ARS Database
Vendor Address	ARS Database
UNIX Schema	**Data Source**
Device Hostname (key field)	User Entry
Vendor (key field)	ARS Database
Model Number	ARS Database
Vendor Phone	ARS Vendor Schema
Vendor First Name	ARS Vendor Schema
Vendor Last Name	ARS Vendor Schema
Device Physical Location	IT/O
Device Status	IT/O
Expiration date of warranties	ARS Database
Action Requests	ARS Rule
Hub Schema	**Data Source**
Board Serial Number (key Field)	ARS database
Board Type	ARS database
Software Revision Level	ARS database

2.2.2.3 HP NetMetrix

The NSM must supply a performance monitoring tool to provide capacity planning capabilities and trend analysis of NCC resource usage. This tool must have the ability to collect, integrate, and correlate data on each segment of the NCC98 network. It should be able to show bandwidth utilization traffic throughout the NCC, provide easy reporting capabilities, and locate network bottlenecks. Additionally, because the networking devices (hubs) have not been identified, it must be flexible enough to gather data from either a hardware probe, to be deployed on each segment, or from RMON-capable hubs. HP NetMetrix meets these criteria and is the tool recommended for the NSM.

HP NetMetrix provides the ability to collect, integrate, and correlate data on each segment of a network through HP LanProbe units or RMON-capable hubs. It consists of eight major modules: Internetwork Monitor, Reporter, Internetwork Response Manager, Load Monitor, Protocol Analyzer, Network File System (NFS) Monitor, Traffic Generator, and Enterprise Utilities. The Internetwork Monitor module collects data from individual segments on the network and can display both detailed and summary utilization reports. Traffic can be analyzed and broken down between individual nodes. Additionally, the Traffic Profile Modeler module allows operators to conduct "What-If" scenarios to optimize network performance.

HP NetMetrix's Reporter module provides reporting capability of the collected data. It can be configured to generate automatic reports on network resource utilization. Historical data can be archived and later retrieved for trend analysis. It also supports the RMON standard (RFC 1215) to produce network health profile reports.

The Internetwork Response Manager (IRM) can generate notifications to operators in the event that a device responds abnormally, indicating a potential trouble spot. The Load Monitor lets NCC operators examine traffic patterns by source, destination, node conversation partner, protocol type, packet size, and segment statistics over time. It provides all seven layer ISO analysis and tracking, even across the application layer. The Protocol Analyzer module provides continuous capture, decode, and display of all protocol layers of internetwork packets in real time, assisting in centralized troubleshooting and analysis at the network level.

HP NetMetrix also provides some network modeling and test features. The Traffic Generator can generate a precise traffic profile to simulate load on the network or test network devices. The Traffic Profile Modeler segment of the Internetwork Monitor allows operators to conduct "What-if" scenarios to optimize network performance.

Finally, HP NetMetrix can augment Fault Management capabilities by offering enterprise-wide configuration of RMON threshold alarms with the Enterprise Utilities module. SNMP-based alarms can be forwarded to a variety of SNMP management platforms. HP NetMetrix is available in a variety of options, and the end-user can choose which modules are needed for the network.

2.2.2.4 HP Omniback II

The NCC is comprised of multiple heterogeneous platforms, both UNIX-based and legacy systems, that run a variety of software. It must provide reliable and continuous service to end-users. As such, it requires a high performance backup and restore capability of both server operating systems and volatile NCC databases. This capability can be met with HP Omniback II.

HP OmniBack II provides centrally managed, enterprise-wide backup and restore capabilities across multi-vendor distributed computing environments such as the NCC. The product also offers automated, reliable, and high performance network backup and restore in combination with a sophisticated media management. High system availability and easy management of large volumes of media and data are provided as well.

Omniback II provides centralized installation, administration, and monitoring for all backup tasks and allows for an enterprise-wide centrally managed and policy driven backup strategy. Omniback II provides security for sensitive data and allow for end-user restore capabilities through configurable user access control mechanisms, user access privileges, and scheduled backups.

OmniBack II has the following features:

- Fast parallel backup to high capacity backup devices
- High system availability even with large volumes of data
- Unattended “lights out’ operation
- System security for sensitive data
- Integrated file system and raw disk backup
- Central administration over WAN and LAN
- Database backup using current on-line backup API’s
- Agent for integration with OmniStorage and SAP/R3
- Works with a range of tested peripherals, including autochangers from Exabyte, ADIC Spectralogic, and Storagete.

OmniBack II offers support for HP-UX and minimizes the consumption of network bandwidth. It provides local backup for the mixed UNIX system environment. NCC operators will be able to schedule and manage all of their backup activities from one central location. A notification feature gives users an easy and quick overview of all systems configured in the environment. OmniBack II also provides information on all backup and restore sessions, allowing end users the ability to verify that their data is protected.

OmniBack II’s run-rate performance is more than 20GB/hour for a single drive. It allows read and write capabilities to multiple disks from one backup drive at a time. OmniBack II is scaleable, easy to use, powerful, and will provide reliable backup service for NCC98.

2.2.2.5 BGS BEST/1 Performance Monitoring

Due to the mission-critical nature of the NCC, it is imperative to monitor the performance of NCCDS system resources, particularly the SPSR database and critical system processes. The NSM must provide real-time monitoring of system level performance, including I/O activity, CPU utilization, and other system resources. Additionally, it must monitor database activity to inform operators of potentially harmful conditions before they cause problems. It must integrate with the HP OpenView framework by sending SNMP traps to notify operators of critical conditions. Finally, the system monitoring tool must have the ability to operate in a heterogeneous environment, supporting multiple UNIX variants as well as legacy VAX systems. BGS BEST/1 Performance Suite meets all of these criteria and is the tool recommended for NCC98. BEST/1 consists of three components that provide real-time process monitoring, trend analysis, and "what-if " modeling techniques: BEST/1-Monitor, BEST/1-Predict, and BEST/1-Visualizer.

BEST/1-Monitor can detect and act on system performance exceptions. BEST/1-Monitor has two components: the BEST/1-Monitor console, which is an object-oriented Motif-GUI, and the BEST/1 Configurable Agents, that reside on the managed systems. The BEST/1 Configurable Agents can be customized to detect errors or exceeded thresholds in processes specified by the operator. Using the BEST/1-Monitor console, the operator can set notification and display policies for any managed device or group of managed devices across the enterprise. BEST/1-Monitor sends SNMP traps based on configurable BEST/1 conditions to both the BEST/1-Monitor console and IT/O. It provides the capability of logging events for later analysis and real-time graphical display of configurable BEST/1 metrics.

The BEST/1-Visualizer component provides trend analysis and graphical display capabilities for system performance data gathered by BEST/1 Configurable Agents. Trend reports and utilization graphs can be generated either automatically or on demand. The BEST/1-Visualizer runs on a PC and can be set up to run in either a standalone mode or integrated with the BEST/1-Monitor console.

BEST/1-Predict provides modeling capability based on past performance for managed systems. It can be used to test new applications under historical loads, provide capacity planning information for future expansion, and model entire systems. The systems model will incorporate CPU, I/O, memory, and response time based on the entire system rather than limited metrics on individual systems.

The BEST/1 Performance Suite has agents for HP-UX 9.x and 10.x, Sun Solaris 2.x and 1.x, as well as OpenVMS. It will provide excellent performance monitoring capabilities across all managed systems used by the NCC.

2.2.2.6 Spider

The NSM has a requirement to maintain all of the NCC98 configuration files in an Oracle database. These files must be easily accessible and easy to edit. Spider, a robust Web-to-database application from Spider Technologies, integrates graphical/visual development with a high-performance deployment engine. NCC Operators will be able to easily and quickly create and maintain NCC98 configuration files using this Web-to-database application.

Spider is a robust Web-to-database interface application that provides a drag-and-drop development capability to create SQL-based query forms. These forms can be displayed in a standard HTML browser. Spider provides a Common Gateway Interface (CGI) application gateway between the Spider-created SQL form and an RDBMS such as Oracle.

The Spider solution consists of two parts: a development module for creating applications in a visual development environment, and a deployment module for the execution of applications that are built in the visual environment. These two components allow the Spider Web-to-database application to deliver high performance, scaleability, and reliability.

Spider is based on an object-oriented architecture that makes it extremely easy to support new technologies in user interfaces, such as JAVA and PDF, as well as databases. It provides a migration path to new technology, protecting the investment in hardware and software. The Spider solution also provides reporting on the usage and load of the Spider application, in order to better manage the application and its configuration.

Spider provides continuous access of its deployment module to end-users, regardless of the licensing configuration on the Oracle database. It queues and schedules requests from end-users via a request broker, so that if all of the concurrent database connections are being used, the request simply waits until a connection is available. Additionally, Spider integrates a system monitor that tracks dying processes and restarts them, ensuring high availability of the Spider system.

Spider will simplify the management of NCC98 configuration files by allowing the NSM Administrator to create and edit HTML compliant SQL-query forms in an intuitive drag and drop, point and click environment, without programming. The NCC Operators will be able to build and maintain configuration files with Spider using a simple HTML viewer. Spider is the tool recommended for the NSM to assist in Configuration Management.

2.2.2.7 Oracle

The NSM requires a database which has the capability to store large volumes of data for efficient update and retrieval between multiple clients. The database server must not negatively impact critical database applications that the NCC depends on to fulfill its mission. To ensure that critical NCC databases suffer no performance degradation, a separate NSM relational database management system (RDBMS) is necessary. Oracle is the database of choice due to its manageability, integration, flexibility, and distribution capabilities.

The Oracle RDBMS provides a proven database technology to the NCC. Its relational database technology provides the foundation of an overall distributed computing solution, enabling database servers to share data in many different ways. Data can be shared on a real-time, or synchronous, basis to ensure application integrity and minimize complexity. Data can also be shared on a deferred, or asynchronous, basis maximizing availability and response time.

The Oracle database system provides management tools that integrate with external GUI-based client applications. It has the ability to meet large data storage requirements. Some key features include the following:

- Supports all forms of distributed data sharing, direct remote access and replication, synchronous real time operations, and asynchronous deferred operations.
- Provides management tools and distributed features that are automatic, transparent, and robust to handle the demands of the organization
- Optimizes performance and is easy to use.

2.3 NSM Detailed Functional Area Support

As stated previously, the proposed NSM solution will be based on a central network and systems management platform consisting of integrated hardware and software components detailed above. This section describes in detail how the tools integrate to meet the NCC98 NSM functional requirements.

2.3.1 Accounting Management

According to the *NCC98 SRD 1998*, the NSM has the requirement to track account activity, provide message and event logging, and maintain an audit trail. This information includes:

- Suspicious network activity for the firewall and NPG
- System generated reports for all managed subsystems
- Record of currently logged on NSM operators
- Network status and statistics.

To accomplish these goals, the NSM will integrate the following tools: BGS BEST/1 Performance, HP NetMetrix, and IT/O. These tools provide Accounting Management functionality in the following way.

As the integration framework, IT/O will be responsible for gathering statistics information in a central location that can be easily accessed. Statistics will be collected from BEST/1 Configurable Agents, IT/O Intelligent Agents, and general SNMP agents. Data collection will be performed by all three tools.

HP NetMetrix will provide both automated and on-demand reporting capabilities for network resource utilization. BEST/1 provides reporting capabilities for systems resource utilization statistics. The reports can be displayed on the NSM client console or printed out in hardcopy.

IT/O can be used to maintain a record of currently logged on users. Additionally, it can be customized to provide information regarding suspicious activity on managed nodes via the IT/O Intelligent Agent.

2.3.2 Configuration Management

The *NCCDS SRD 1998* specifies a number of detailed requirements related to some form of configuration management. These requirements include such items as:

- Specify and maintain NCC system and network configuration files;
- Provide X-terminal bootup configuration files; and
- Monitor, update and control connectivity of individual subsystems to the OpsLAN.

Configuration management is complex and requires many capabilities. To achieve these goals, the NSM will integrate the following tools: Spider, Oracle, Netscape Navigator, HP-UX, and IT/O.

IT/O provides limited configuration management capabilities. It provides a centralized location to maintain a unique list of IP addresses in current use. It will also track network service ports as needed. Additional bootup configuration files can be maintained and distributed through HP-UX's native BOOTP daemon.

To provide startup, shutdown, and configuration of NCC98 subsystems, the NSM will incorporate Spider, a Web-database application, into its platform. Using Spider, the NSM Administrator can easily create an SQL query form that can be read by any HTML viewer. The resulting SQL query form will be used by NCC operators to edit and maintain all of the NCC98 configuration information in an Oracle database. These forms can be printed, deleted, or modified by the NCC operator. Spider also allows for access restrictions to certain forms to maintain security.

At the present time, it is not possible to define what type of LAN configuration management will be possible due to the fact that a final selection of the COTS hubs to be used in NCC98 has not been made. If an appropriate COTS switching hub is selected and management software is available for the chosen hub, it should be possible to obtain physical configuration information directly from the switch caches resident in the hubs. However, this may not be possible if the hub manufacturer does not provide the appropriate information through its SNMP agent or its management software. Therefore, the NSM architecture cannot specify how LAN configuration management requirements may be met.

2.3.3 Fault Management

According to the *NCCDS SRD 1998,* the NSM subsystem must provide the immediate capability of detecting, notifying, and resolving errors within the NCC system. This capability is known as Fault Management and includes such items as:

- 24 by 7 monitoring of OpsLAN;
- Notification of errors; and
- Automatic failover from primary to backup systems.

Fault Management requirements for NCC98 will be coordinated through IT/O but will require the integration of three third-party applications: Remedy ARS, HP NetMetrix, and BEST/1-Monitor.

IT/O automatically performs status polling across its managed domain. When a managed node fails to respond to a node, IT/O records that event in its event log. Additionally, IT/O acts as the SNMP manager and will receive SNMP traps from the performance monitoring tools, HP NetMetrix and BGS Best/1-Monitor. Where possible, the network hubs will be configured to forward SNMP traps to IT/O. When IT/O receives an SNMP trap, it logs it into its event log and can be configured to display a notification dialog on the NSM workstations. However, to improve problem tracking capabilities and provide better notification mechanisms, the NSM team will integrate the Remedy ARS trouble-ticketing tool with IT/O.

Remedy ARS will reside on the NSM server and intercept all events and SNMP traps in the event log maintained by IT/O. It will be configured to generate a trouble ticket when IT/O receives specific events. Upon receiving an event, ARS will update its Oracle database, retrieve the appropriate schema, populate it with information directly from IT/O, and notify the appropriate NCC personnel. For critical events requiring immediate action, ARS will provide multiple notifications including dialog display at the console, e-mail, and paging. For less critical events, ARS will provide a more basic notification to the operator in a manner to be determined at implementation.. Examples of events that will cause ARS to generate a trouble ticket include:

- Critical SPSR process not running or exceeds set CPU threshold;
- SPSR database full or percent space exceeded;
- SPSR temporary database full or percent exceeded;
- Critical NPG process not running or exceeds CPU threshold;
- Critical NPG MIB value exceeds threshold. This depends on the specific MIB that will be written by the NPG design team;
- SPSR failover event initiated by SPSR failover product;
- NPG failover event initiated by NPG failover product; and
- Critical node or hub failure to respond to status poll.

2.3.4 Performance Management

Performance Management needs for NCC98 is required by the *NCCDS SRD 1998*. These requirements will be met through the integration of several tools into the IT/O framework. These tools are: HP NetMetrix and the BGS BEST/1 Performance Monitor suite.

To accomplish performance management goals for NCC98, it is necessary to collect statistics and utilization data in two separate areas: network resources and systems resources. HP NetMetrix provides superior performance monitoring for network resources, while BGS BEST/1 provides excellent performance monitoring for all of the heterogeneous systems and proprietary processes in use by the NCC.

At the present time, it has not been determined what type of network hubs will be used to segment the NCCDS LANs into the four separate LANs to be used by Test, Operations, and Development, Test, & Training (DT&T). The collection of network performance data requires either one of the following:

1) RMON-compliant hubs with network management modules (NMMs) installed; or

2) Individual hardware probes such as the HP LANProbe III deployed on each LAN.

This requires a flexible solution using a COTS tool with the capability to collect data from either source. HP NetMetrix will be used as the data collection utility through its Internetwork Monitor module. Data to be collected will be stored for a limited period in HP NetMetrix flat-file format. Data collection will be performed on a variety of variables, including, but not limited to, the following:

- Node-to-node, source-to-destination traffic across segments;
- Ethernet and token-ring performance metrics such as network bandwidth utilization, packets, octets, broadcasts, and error types across LAN segments; and
- RMON history group information, providing TopN reports, protocol distribution, traffic characteristics, host/conversation bandwidth, or application layer with relative comparison to overall bandwidth consumption.

HP NetMetrix will be integrated into the IT/O client console to provide easy operator access to network performance information.

In the systems area, the BEST/1 Performance suite will be used to provide monitoring of critical processes and system health. The BEST/1-Monitor console will reside on the NSM server located in the NCC. BEST/1 Configurable Agents will be deployed on each of the managed systems: SPSR server, NPG, Firewall, SPSR workstations, and CCS VAX. These agents will be configured with a list of specific critical processes to monitor for each managed system. Each agent will also monitor a set of standard system resource processes including, but not limited to, CPU utilization, I/O activity, and networking parameters. Additionally, the BEST/1 database agent will be installed on the SPSR server to monitor performance of the SPSR database. This agent will notify NCC operators in the case of critical events on the SPSR database.

The BEST/1-Monitor console will be configured to forward BEST/1 alarms to the IT/O framework for notification of systems events. The BEST/1-Monitor console can be accessed from any of the NSM workstations or server.

Once performance data is collected from the NCCDS subsystems, it will be necessary to display the information in a concise format. Both HP NetMetrix and BEST/1-Visualizer offer graphing and visualization tools to display both real-time and historical data. Both products can be configured to automatically produce utilization reports at regular intervals. Additionally, they can be used to generate reports and provide network and systems modeling capabilities based on past data. These features will assist both network and systems planning personnel in capacity planning exercises, as well as providing invaluable data to the Integration Test and Acceptance Test teams during the testing process.

2.3.5 Security Management

The *NCCDS SRD 1998* includes requirements for monitoring security on the NCCDS LANs. These considerations for the NSM include authentication, access control, and audit trails. These features will be implemented using a combination of IT/O and functionality inherent in UNIX operating systems. The *NCCDS SRD 1998* requires that an NCCDS user must be uniquely identified and validated before being granted access to the NCCDS system or resources.

To meet this requirement, each NCC system will employ separate security measures to ensure that NCC data is not compromised. Each system will have a number of users, each with a unique password. Each user will have different access rights to different NSM tools, NCC databases, and NCC subsystems. The UNIX username and password is the first line of security into the NCC systems to prevent unauthorized access. To provide further security restrictions, UNIX file access privileges can be defined according to task needs.

Additionally, NSM security measures must safeguard critical devices within the NCC, specifically the NSM itself, access privileges on NCCDS subsystems, and the interaction of the NSM with managed devices. The security measures described herein are not meant to provide overall network security to all devices on the network, but provide limited logging and detection of unauthorized access attempts. IT/O will serve to provide security management capabilities for account privileges and file permissions on the enterprise.

In addition to unauthorized access logging provided by the HP-UX operating system, IT/O provides security reports to indicate any invalid login attempts. The system will terminate any login attempts that are deemed illegal. It allows message conditions to be set up to trap logins, legal or illegal, and disconnects them upon an indication of non-availability for the attempted login. Further security features are provided through access controls which restrict the user to limited system resources.

2.3.6 General Systems Management

Although General Systems Management is not a standard OSI functional area, it has been defined to include infrastructure requirements for a comprehensive NSM architecture. General

Systems Management concerns issues such as SNMP configuration, customization, and backup and restore functionality.

The integration of two COTS tools, in conjunction with features of the UNIX operating system, will be utilized to provide the infrastructure necessary to support an enterprise-wide NSM function across distributed platforms. These tools are HP IT/Operations and HP Omniback II.

IT/O has the ability to manage all elements within an enterprise through intelligent agents resident on each managed node. This feature enables centralized management across the enterprise, giving an NCC Operator the ease of what appears to be one homogeneous computing environment. It includes centralized account administration and maintenance of local DNS server processes.

The NCC operator will control central account administration using the UNIX-standard Network Information Systems (NIS), formerly known at Yellow Pages (YP). An NIS database will reside on the NSM server to provide a single location to add, delete, and modify accounts on the NCC UNIX systems. The other NCC UNIX systems will be configured as NIS clients, obtaining user account information from the NSM server.

The NCC98 system backup and restore capabilities will be provided by the HP OpenView OmniBack II application. HP Omniback II has the automated, reliable, and restore capabilities to meet the demands of the systems management requirements. The NSM will provide nightly incremental backup capabilities to all of the NCCDS systems and databases, utilizing a high-capacity tape drive residing on the NSM server. HP Omniback II client software will be installed on all NCCDS systems, excluding legacy systems, allowing for remote, automated backup capability. Automated full backups of critical NCCDS systems will also be performed regularly, although the optimal full backup interval has not been determined at this time.

3. Costs

3.1 Introduction

This section outlines the cost of each NSM architecture component. Procurement for the NSM architecture will be coordinated through the existing Scientific Engineering Workstation Procurement (SEWP) contract, where applicable. If a specified NSM architecture component is not available through the SEWP, a standard GSA estimate will be supplied unless otherwise stated.

3.2 Hardware

The NSM hardware components and the associated costing information are supplied in this section. An itemized break down for each component and the necessary add-ons are also provided. Table 3-1 indicates the total costs for the hardware components of the NSM architecture. Vendor price at a Government Service Agreement (GSA) discount is indicated only when SEWP price is unavailable. The Pricing Option column indicates an S for the SEWP contract and a V for Vendor supplied costs.

Table 3-1 Hardware Components

Hardware	Pricing Option	Cost	Qty	Total Cost
• **HP 9000 J-Class Workstation Model J210**				
HP Model J210 HCRX-8 Workstation,				
20” Color, 128 MB RAM, 4 GB Fast-Wide Disk	S	$ 34,133	1	$ 34,133
+ 4GB DSS2 DAT Tape Drive	S	2,695	1	2,695
+ 2GB disk drive, FWD SCSI-2	S	1,350	1	1,350
+ 4X CD-ROM drive, SCSI -2	S	500	1	500
Total cost of workstation				**$ 38,678**
• **HP 9000 C-Class Workstation Model C100**				
HP Model C100 HCRX-8 Workstation,				
20” Color, 32 MB RAM, 2 GB Disk	S	$ 16,725	4	$ 66,900
+ 3 32MB ECC memory modules	S	6,240	4	24,960
+ 4X CD-ROM drive, SCSI-2	S	500	4	2,000
Total cost of workstations				**$ 93,860**
Total Hardware Costs				**$132,538**

3.3 Software

The NSM COTS Tools and their associated cost are described in this section. If a particular product requires several components, the component price is listed also. Table 3-2 indicates the total costs for software components of the NCCDS and NSM architecture. Vendor price at GSA discount is indicated only when SEWP price is unavailable. The Pricing Option column indicates an S for the SEWP contract and a V for Vendor supplied costs.

Table 3-2 Software Components

Software Costs	Pricing Option	Cost	Qty	Total Cost
• **HP IT/Operations**				
HPIT/O License to Use (LTU) Management Server	V	$ 31,200	1	$ 31,200
HP IT/O LTU Client Workstation	V	386	4	1544
HP IT/O Media for managed Nodes	V	230	1	230
Total HP IT/O				**$32,974**
• **Remedy ARS**				
Remedy ARS Server	V	$ 9,500	1	$ 9,500
Remedy ARS Client	V	$ 2,000	4	8,000
Total Cost of Remedy ARS				**$ 17,500**
• **HP NetMetrix**				
HP NetMetrix/UX Enterprise Manager	V	$ 23,085	1	$ 23,085
HP NetMetrix/UX Media/Documentation Kit	V	$ 1,440	1	1,440
LANProbe III Plus/Ethernet Monitor w/AUI	V	$ 2,895	2	5,790
Total HP NetMetrix				**$ 27,420**
• **HP OmniBack II**				
HP 9000 OmniBack II Manger for Series 700	S	$ 1,900	1	$ 1,900
HP 9000 OmniBack II Backup Node	S	150	3	450
Total HP OmniBack II				**$ 2,350**

Table 3-2 Software Components, cont.

Software Costs	Pricing Option	Cost	Qty	Total Cost
• **BGS Best/1**				
HP C100 Agent License	V	$ 433	5	$ 2,165
HP J210 Agent License	V	2,165	1	2,165
HP K200 Agent License	V	3,465	1	3,465
HP Console License	V	22,560	1	22,560
Oracle Console License	V	5,640	1	5,640
Oracle Agent License	V	1,917	1	1,917
VAX License	V	26,419	1	26,419
Total BGS Best/1				**$64,331**
• **Spider Technologies Spider**				
Spider WWW browser	V	$ 3,146	1	$ 3,146
Support	V	749	1	749
Total for Spider				**$ 4,495**
• **Oracle 7 RDBMS**				
Oracle, UNIX Server Bundle, 8 concurrent user	S	$ 9,374	1	$ 9,374
Oracle, UNIX Server Based Tools Bundle	S	$ 1,166	1	1,166
Oracle, UNIX Networking Bundle	S	347	1	347
Oracle, UNIX Client Based Tools Bundle	S	$ 1,166	1	1,166
Total cost for Oracle 7 RDBMS				**$ 12,053**
• **Netscape**				
Netscape Server	S	$ 1,421	1	$ 1,421
Netscape Navigator Client 2.x	S	35	4	140
Total cost for Netscape				**$ 1,561**
Total Software Costs				**$ 162,684**
Total Hardware and Software Costs				**$ 295,222**

4. Interface with NCC98 Subsystems

4.1 Introduction

This section of the NSM Architecture provides a description of the interface between the NSM and the NCC98 subsystems. Each interface is unique due to the fact that each subsystem must provide specific network and systems information to the NSM. Additionally, each subsystem may require a particular response from the NSM.

4.2 SPSR Subsystem

The NSM will interface with the SPSR to provide database monitoring, database backups, and database performance statistics. The NSM will also monitor the stability of specific SPSR processes, perform status polling on the SPSR servers and workstations, and gather system statistics through intelligent agents resident on the SPSR systems. Additionally, the NSM will provide configuration information and interface with the high-reliability software installed on the SPSR server to coordinate failovers and inform NCC Operators that a failover has occurred.

SPSR hardware consists of an HP K Class server running HP-UX 10.X, a UNIX operating system. The NSM will utilize the IT/O platform to monitor the SPSR database and associated SPSR processes.

To meet its requirements, the NSM will need to be supplied with the following information from the SPSR subsystem:

- List of critical processes to be monitored;
- Scripts to allow remote startup and shutdown of the SPSR systems or an appropriate Management Information Base (MIB) instance and associated SNMP agent to allow remote startup and shutdown;
- Interface with the high-reliability failover software to allow the NSM to detect and/or initiate failover of the SPSR system;
- Trivial File Transfer Protocol (TFTP) access to the SPSR servers and workstations to allow transfer of SMTP configuration files on system startup; and
- TFTP requirements for the SPSR workstations to permit the NSM server to act as a BOOTP server to the SPSR workstations.

4.3 CCS Subsystem

Because CCS operates on a legacy VAX running Open VMS, the NSM will provide only generic management capabilities to the CCS processes. No startup and shutdown capabilities will be possible for CCS. In order to provide NSM services to CCS, NSM will require the following:

- SNMP-compliant agent resident on the CCS VAX and its associated VMS MIB definition from Digital; and
- List of critical processes to be monitored by the BEST/1 Configurable Agent for OpenVMS.

The only additional NSM services that will be provided to CCS is status polling of the VAX itself.

4.4 NPG

The NPG requires startup configuration information in addition to process and statistics monitoring capability. Additionally, the NSM will interface with the high-reliability software installed on the NPG server to coordinate failovers and inform NCC Operators that a failover has occurred.

To provide these capabilities, the NSM will require additional information from NPG. Necessary information includes:

- List of critical NPG processes to be monitored;
- MIB definition specific to the NPG supported by an NPG SNMP agent. This MIB definition should include standard routing statistics such as NumPacketsIn, NumPacketsOut, %MemoryUtilization, NumCollisions, NumPacketsDropped, CRCErrors, and any other statistics that are needed to monitor the NPG;
- Interface to the specific failover package to allow the NCC Operator to detect and/or initiate a failover event;
- TFTP access to the NPG server to allow transfer of NPG configuration files; and
- MIB definition to allow the NPG to interrupt a process, re-read a configuration file, and restart the process.

The NSM will provide status polling information to detect whether the NPG server responds to a ping.

4.5 Firewall

Due to security implications, the Firewall is a special case. Monitoring can take place only on the interior interface to the Firewall machine, and it is not clear at this point what monitoring will be available. An SNMP agent may violate security requirements, and the commercial Firewall package may have its own monitoring software. If that is the case, the NSM will need an interface to read any log files or traps produced by the Firewall software. Otherwise, the NSM will provide only status polling capabilities regarding the Firewall.

4.6 LAN

From a high-level standpoint, the NSM will be able to provide status polling information to all IP devices on the LAN. An eventual goal of the NSM is to provide LAN configuration information, but it can only be met if the COTS hub that is selected for NCC98 supports LAN configuration changes through vendor-specific software. Because the COTS hub that will be used has not yet been selected, it is premature to specify exactly how the NSM will monitor LAN configuration information.

LAN utilization statistics information can be provided to the NSM in one of two ways. In the first, the selected COTS hub will be RMON-capable with supported agent software to gather RMON statistics and send them to an SNMP manager. In the second, hardware probes will be deployed on each LAN to monitor traffic on the LAN. HP NetMetrix will be used to read either the RMON information stored on the hubs or LAN statistics provided by the probes.

5. Conclusion

The proposed NSM architecture described in the preceding pages will support NCC98 goals by preventing network and system faults from adversely affecting NCC operations while maintaining the highest level of services to users. By providing a means to monitor system resource utilization, NSM will enable NCC operators to detect and isolate faults and potential problem areas before they affect end-users. The use of existing standards ensures compatibility with future products adhering to network and systems management standards. Additionally, the centralized architecture provides a single point from which to monitor and troubleshoot NCC operations, greatly streamlining functionality.

The NSM architecture is comprised of Commercial Off-The-Shelf (COTS) tools which accurately meet the stated functional requirements. The recommended tools represent the best of breed for each OSI management category. Various high-level evaluation criteria included as part of the tool selection process included integration with management platform, available functionality, end-user graphical user interface, future direction/overall product strategy, and compliance with open standards.

Proactive notification and monitoring of critical NCC subsystems that is provided by NSM will greatly enhance the services offered by the NCC. Because of current and future changing technology, it is important to provide redundant fail-safe features to ensure services to end-users utilizing state of the art systems. NSM features will assist in positioning NASA for efficient use of current technology and the ability to make use of future developments as they occur, making the NCC more technology adaptable, more reliable, and able to guarantee customer service restoral levels.

It should be noted that a comprehensive Concept of Operation integrating the end-user community with the NSM solution is a necessity ensuring successful operational transition. An NSM Concept of Operation was not included within this task due to agreed upon original statement of work. The NSM Concept of Operations will identify interaction processes and procedures between NCC personnel and NSM solution. Interface specifications will identify items such as functionality available to each end-user NCC group, unscheduled event resolution process, network/system prioritization scheme, service restoral levels, and escalation/status procedures.

Appendix A. Validated Functional Requiremenbts

A.1 Introduction

Appendix A presents the validated functional requirements for the NSM subsystem of NCC98. The validate functional requirements have been derived from a combination of interviews with key NCC98 personnel and directly from the NCCDS SRD 1998. The requirements are grouped according to OSI network and systems management standard functional area.

The subsequent tables in this section contain the following columns: Requirement Number, Requirement, Source, and COTS Tool. These columns are defined below:

- Requirement Number—the number assigned by the NSM Design Team to the requirement. It has no relation to any previous NCC98 document.
- Requirement—the text of the requirement, sometimes paraphrased from the original requirement as it appeared in previous NCC98 document.
- Source—the original source of the requirement. This may be any of the NCC98 System Requirements Document (SRD), NCC98 System Design Specification (SDS), or personnel interviews.
- COTS tool—the tool selected by the NSM Design Team to fulfill the requirement. Requirements that state CUSTOM or HP-UX 10.x in the COTS Tool column are those requirements that are implemented through the HP Operating System or custom built software.

A.2 Accounting Management

The requirements stated in this section are the Accounting Management functional requirements. Table A-1 below defines the functional requirement number, functional requirement, its source: and the COTS tool which will satisfy the functional requirement.

Table A-1. Accounting Management Functional Requirements

Req Number	Requirement	Source	COTS Tool
NSM-1	The NSM shall provide a report generation function to produce reports. The data used as the basis for these reports may be retrieved from the historical log	SRD 8.3-8.4	NetMetrix, BEST/1
NSM-2	The NSM shall provide configuration storage, SNMP statistics, information on suspicious activity, etc., for the firewall and gateway.	Interview	ORACLE 7, NetMetrix, IT/O
NSM-3	The NSM shall maintain a record of currently logged-on operators.	SRD 9.3.6	HP-UX 10.X
NSM-4	The NSM shall log external messages. Still open?	SRD 8.2.2.1.A.2	CUSTOM

A.3 Configuration Management

Configuration Management provides the ability to manage NCC98 assets and enforce system-wide network and systems standards. Table A-2 defines the Validated Functional Requirements that will be met by the NSM.

Table A-2. Configuration Management Functional Requirements

Req Number	Requirement	Source	COTS Tool
NSM-5	The NSM shall provide centralized configuration management and control of routing tables, scheduled failovers, and software versions.	Interview	SPIDER, ORACLE 7, IT/O
NSM-6	The NSM shall provide the operator with the capability of modifying and verifying the current operational NCCDS system configuration via an interactive display	SRD 9.3.6	SPIDER, ORACLE 7, Netscape Navigator, CUSTOM
NSM-7	The NSM shall provide the capability to automatically reconfigure the system configuration in the event of a fault or failure.	SRD 9.5.2.4.A	SPIDER, ORACLE 7, CUSTOM
NSM-8	The NSM shall provide the operator with the ability to enable or disable the automatic reconfiguration.	SRD 9.5.2.4.C	SPIDER, CUSTOM
NSM-9	The NSM shall provide the operator with the capability of specifying the NCCDS system configuration that will be effective as of system startup.	SRD 9.5.2	SPIDER, ORACLE 7, CUSTOM

Table A-2. CM Functional Requirements Cont.

Req Number	Requirement	Source	COTS Tool
NSM-10	The NSM shall provide a database to maintain system configuration status, to establish and maintain operators' accounts, and to monitor and control system security.	SDS 4.2.1.3	ORACLE 7
NSM-11	The NSM shall monitor and control the connectivity and status of the OpsLAN. The NSM shall interface with the NACC to configure the physical connection among the NCCDS nodes.	SDS 4.2.1.3	IT/O
NSM-12	The NSM shall provide system configuration tables to specify the initialization server, setup parameters, and kernel software via TFTP for x-terminal startup.	SDS 4.2.1.3	HP-UX 10.x
NSM-13	The NSM shall provide system configuration tables to specify the session establishment servers for x-terminals.	SDS 4.2.1.3	HP-UX 10.x
NSM-14	The NSM shall provide the capability of selecting a configuration for NPG initialization.	Interview	SPIDER, CUSTOM
NSM-15	The NSM shall provide the NPG (protocol conversion gateway) with its initial configuration information of transport end point definitions.	SDS 4.2.1.2	SPIDER, ORACLE 7, CUSTOM
NSM-16	The NSM shall interface with the NPG to establish and maintain transport end point definitions.	SDS 4.2.1.3	IT/O, SPIDER, ORACLE 7
NSM-17	The NSM shall provide a database to store configuration information on the NPG process.	Interview	ORACLE 7
NSM-18	The NSM shall maintain system performance information.	SRD 9.5.2.5.C	BEST/1, NetMetrix, ORACLE 7
NSM-19	The NSM shall interface with DNS and NIS to establish and maintain host IP addresses, process protocol port numbers, and mapping of meaningful process names and addresses.	SDS 4.2.1.3	IT/O
NSM-20	The NSM shall maintain UDP and TCP protocol port numbers.	SDS 4.2.1.1.3	IT/O
NSM-21	The NSM shall provide electronic-mail configuration files for the SPSR server and workstations	Interview	IT/O
NSM-22	The NSM shall interface with the NACC or other switching device to control the connectivity configuration of the NCC network.	SDS 4.2.1.1	IT/O

A.4 Fault Management

Fault Management is the process of detecting, isolating, and correcting abnormal network and systems operations. A fault results from the failure or degradation of a system, application, process, circuit, or device. Table A-3 below defines the Validated Functional Requirements for NCC98.

Table A-3. Fault Management Functional Requirements

Req Number	Requirement	Source	COTS Tool
NSM-11	The NSM shall monitor and control the connectivity and status of the OpsLAN. The NSM shall interface with the NACC to configure the physical connection among the NCCDS nodes.	SDS 4.2.1.3	IT/O
NSM-23	The NSM shall provide 24 x 7 capability of monitoring the status of all IP and/or SNMP compliant components, providing the operator with immediate access to information needed for the resolution of the event.	Interview	IT/O
NSM-24	The NSM shall coordinate failovers between NCCDS systems and interface with COTS failover tools installed on NCCDS systems.	Interview	?????
NSM-25	The NSM shall notify the NCC operator if the internal resource usage of critical devices and/or processes exceeds a pre-determined level.	Interview	ARS, IT/O, BEST/1
NSM-2	The NSM shall provide configuration storage, SNMP statistics, information on suspicious activity, etc., for the firewall and gateway.	Interview	ORACLE 7, NetMetrix, IT/O
NSM-26	The NSM shall interface with NCCDS segment operating systems and utilities to monitor and control resource status, segment activity, and process location.	SDS 4.2.1.3	IT/O, NetMetrix, BEST/1
NSM-27	The NSM shall automatically detect device and system failure on critical NCCDS systems and shall notify NCC personnel of such events through paging, audible and/or display to remote NCC operators as necessary.	Interview	HP-IT/O, ARS
NSM-28	The NSM shall provide fault management and notification in terms of paging and audible for network and system events.	Interview	IT/O ARS
NSM-29	The NSM shall provide the capability of automatically reconfiguring the NCCDS to recover from system faults and failures.	SRD 9.5.2	SPIDER, CUSTOM
NSM-30	The NSM shall provide the capability of automatic detection of errors in processing, memory utilization, input/output processing, and communication.	SRD 9.5.2	IT/O, NetMetrix, BEST/1

Table A-3. Fault Management Functional Requirements (Continued)

Req Number	Requirement	Source	COTS Tool
NSM-31	The NSM shall automatically detect errors in processing, memory utilization, I/O processing, and communication.	SRD 9.5.2.3	IT/O, NetMetrix, BEST/1
NSM-32	The NSM shall collect and display status on block counts, message counts, CPU and disk utilization, I/O, connections established, and trend analysis.	Interview	IT/O, NetMetrix, BEST/1
NSM-33	The NSM shall log errors in processing, memory utilization, input/output processing, and communication and shall provide the operator with the capability of viewing this information	SRD 9.5.2	IT/O, NetMetrix, BEST/1
NSM-34	The NSM shall maintain a record of the current status of each NCCDS hardware component.	SRD 9.5.2.5.B	IT/O, NetMetrix, BEST/1
NSM-35	The NSM shall provide internal DNS services. External DNS shall be provided through the NASCOM DNS server.	Interview	IT/O
NSM-36	The NSM shall detect failover events and procedures implemented by the "high availability software" COTS tool that will detect the the failure of critical processes on the NPG, take the existing NPG out of service, and start the NPG process on a backup NPG	Interview	SPIDER, ORACLE 7, BEST/1, CUSTOM
NSM-37	The NSM shall have the capability of initiating NPG failover both manually and automatically from the NSM workstation.	Interview	IT/O, SPIDER, ORACLE 7, CUSTOM
NSM-38	The NSM shall notify the NCC operators of NPG failover and shall log the NPG failover event.	Interview	ARS
NSM-39	The NSM shall detect failover events and procedures implemented by the "high availability software" COTS tool that will detect the failure of critical processes on the Firewall, take the existing Firewall out of service, and start the Firewall process on a backup Firewall	Interview	BEST/1, IT/O, SPIDER, ORACLE 7, CUSTOM
NSM-40	The NSM shall have the capability of initiating Firewall failover both manually and automatically from the NSM workstation.	Interview	IT/O, SPIDER, ORACLE 7, CUSTOM
NSM-41	The NSM shall notify the NCC operators of Firewall failover and shall log the Firewall failover event.	Interview	ARS

Table A-3. Fault Management Functional Requirements (Continued)

Req Number	Requirement	Source	COTS Tool
NSM-42	The NSM shall detect failover events and procedures implemented by the "high availability software" COTS tool that will detect the failure of critical processes on the SPSR, take the existing SPSR out of service, and start the SPSR process on a backup SPSR	Interview	IT/O, BEST/1, SPIDER, ORACLE 7, CUSTOM
NSM-43	The NSM shall have the capability of initiating SPSR failover both manually and automatically from the NSM workstation.	Interview	IT/O, SPIDER, ORACLE 7, CUSTOM
NSM-44	The NSM shall notify the NCC operators of SPSR failover and shall log the SPSR failover event.	Interview	ARS
NSM-45	The NSM shall notify an operator whenever a reconfiguration to the NCCDS is performed.	SRD 9.5.2	ARS

A.5 Performance Management

Performance Management provides NCC98 personnel with the ability to measure, analyze, and predict the behavior of network and systems resources. Table A-5 below defines the Validated Functional Requirements that will be met by the NSM.

Table A-4. Performance Management Functional Requirements

Req Number	Requirement	Source	COTS Tool
NSM-52	The NSM shall use the Simple Network Management Protocol (SNMP) to retrieve information on status, statistics, and IP routing tables from Management Information Base (MIB) variables.	SDS 4.2.1.3	IT/O, BEST/1, NetMetrix
NSM-65	The NSM shall monitor the status and internal resource usage of IP and/or SNMP compliant hardware and software components and shall maintain a record of the current status of each NCCDS hardware component.	SRD 9.5.2	IT/O, NetMetrix
NSM-25	The NSM shall notify the NCC operator if the internal resource usage of critical devices and/or processes exceeds a pre-determined level.	Interview	ARS

Req Number	Requirement	Source	COTS Tool
NSM-66	The NSM shall provide trend analysis of performance statistics, including bandwidth utilization and database performance.	Interview	NetMetrix
NSM-67	The NSM monitoring shall not significantlydegrade the NCCDS performance.	SRD 9.5.2.5.D	IT/O
NSM-68	The NSM shall gather performance statistics on the NPG through a proprietary MIB definition that will be developed by the NPG development team.	Interview	NetMetrix
NSM-2	The NSM shall provide configuration storage, SNMP statistics, information on suspicious activity, etc., for the firewall and gateway.	Interview	NetMetrix, IT/O
NSM-69	The NSM shall log internal NCCDS performance data in terms of network performance and limited application performance.	SRD 8.2.2.1.A.1	NetMetrix, BEST/1, ORACLE7
NSM-3	The NSM shall maintain a record of currently logged-on operators.	SRD 9.3.6	HP-UX 10.x

A.6 Security Management

Security Management provides the ability to safeguard proprietary data and ensure system integrity against unauthorized access. Specifically, Security Management is a compilation of network controls and monitoring mechanisms that enforce accountability, assure data integrity, control access, prevent accidental or malicious disclosure, and assure network availability. Table A-6 below defines the Validated Functional Requirements met by the NSM.

Table A-5. Security Management Functional Requirements

Req Number	Requirement	Source	COTS Tool
NSM-70	The NSM shall control access to the system management and database management functions.	SRD 9.5.4.1 9.5.4.2	IT/O, ORACLE 7, SPIDER
NSM-71	The NSM shall restrict operator access to the NPG and Firewall systems. Access restriction shall be based on records of authorized operators and passwords	SRD 9.5	HP-UX 10.x
NSM-72	The NSM shall maintain the integrity of information in its databases and shall maintain the confidentiality of information in its databases.	SRD 10.8	ORACLE 7
NSM-73	The NSM shall provide administrative restriction of the functional capabilities of individual operators.	SRD 10.2.B	HP-UX 10.x

Req Number	Requirement	Source	COTS Tool
NSM-74	The NSM shall provide the NCC console operators with the capability to log on and off of the NSM system.	SRD 9.3.6	HP-UX 10.x
NSM-75	The NSM shall validate log-on.	SRD 9.3.6.4 9.3.6.5	HP-UX 10.x
NSM-76	The NSM shall provide an audit trail.	SRD 10.6	HP-UX 10.x, IT/O, BEST/1

A.7 General Systems Management

To achieve an adequate level of NSM conformance, a number of preliminary requirements must be met. These requirements are general in nature but are necessary to meet one or more needs of the OSI functional areas. General Systems Management requirements concern issues such as SNMP configuration, customization, user account management, and backup and restore. Table A-4 below defines the Validated Functional Requirements met by the NSM subsystem for NCC98.

Table A-6. General Systems Management Functional Requirements

Req Number	Requirement	Source	COTS Tool
NSM-46	The NSM shall provide a centralized management system residing on a single workstation that will, to the maximum feasible extent, perform all system management and database management functions.	SRD 9.5.1.2 9.5.1.3	IT/O
NSM-47	The NSM shall, to the maximum extent feasible, be based on Commercial-Off-the-Shelf packages to limit software development costs. The NSM shall comply with established network management standards including OSI management model and the Simple Network Management Protocol (SNMP)	Interview	IT/O
NSM-23	The NSM shall provide 24 x 7 capability of monitoring the status of all IP and/or SNMP compliant components, providing the operator with immediate access to information needed for the resolution of the event.	Interview	IT/O
NSM-48	The NSM shall provide network and systems management for the following systems: Firewall, Protocol Conversion Gateway (NPG), SPSR (scheduling) process, and OpsLAN.	Interview	IT/O

Table A-6. General Systems Management Functional Requirements (Continued)

Req Number	Requirement	Source	COTS Tool
NSM-49	The NSM shall provide first-priority systems management capabilities for the systems on the OpsLAN and the Test LAN. Other LAN systems will be provided with NSM capabilities on an as-needed basis.	Interview	IT/O
NSM-50	The NSM will provide network and systems management capability for the CCS (VAX) systems and ACRS to be limited to the capabilities of the standard SNMP agents on the CCS and ACRS systems.	Interview	IT/O
NSM-51	The NSM will not provide network and systems management capability for SAS.	Interview	N/A
NSM-52	The NSM shall use the Simple Network Management Protocol (SNMP) to retrieve information on status, statistics, and IP routing tables from Management Information Base (MIB) variables.	SDS 4.2.1.3	IT/O, BEST/1, NetMetrix
NSM-53	The NSM shall be capable of meeting all function, performance, and reliability/maintainability/availability (RMA) requirements associated with the capabilities planned for operational availability during 1998-2001 under planned workload.	SRD 9.8	IT/O, ORACLE 7, SPIDER, BEST/1, NetMetrix
NSM-54	The NSM shall recover from a fault or failure within 5 minutes.	SRD 9.5.2.4.D	IT/O
NSM-55	The NSM will provide a consistent look-and-feel in the consoles, displays, alerts, and reports provided to and entries expected from the operators	SRD 9.2	HP-UX 10.x, IT/O
NSM-56	The NSM workstation shall contain the following functions: data display, data entry, audio and visual alerts, function selection, rapid function selection, windows, text editing, screen print, and interfaces with NCC CCTV.	SRD 9.3.2.2	HP-UX 10.x
NSM-57	The NSM shall provide centralized account management for user accounts, database accounts, user privileges, user processes, and backups.	Interview	IT/O
NSM-58	The NSM design shall ensure the availability of its databases to external processes.	SRD 10.8.C	IT/O ORACLE 7 SPIDER
NSM-59	The NSM shall provide an operator interface for the firewall and gateway systems through a remote session, i.e., telnet or rlogin.	Interview	HP-UX 10.x

Table A-6. General Systems Management Functional Requirements (Continued)

Req Number	Requirement	Source	COTS Tool
NSM-60	The NSM shall provide database services and commercial-off-the-shelf (COTS) tools from an operator workstation.	SDS 4.2.1.3	N/A
NSM-61	The NSM shall retain NCCDS system and performance data as long as necessary for operations.	SRD 5.2.4.7.1	IT/O, ORACLE 7, NetMetrix, SPIDER, BEST/1
NSM-62	The NSM shall provide on-line backup capability for databases and systems.	Interview	OmniBack II
NSM-24	The NSM shall coordinate failovers between NCCDS systems and interface with COTS failover tools installed on NCCDS systems.	Interview	IT/O, CUSTOM
NSM-63	The NSM shall have the capability to stop and start applications.	Interview	SPIDER, ORACLE 7, CUSTOM
NSM-64	The NSM shall provide two types of console operator positions: database analyst position and positions controlled by the database analyst.	SRD 9.2.1	N/A

Abbreviations and Acronyms

ACRS	Automatic Conflict Resolution System
API	Application Programming Interface
ARS	Action Request System
BB	Bit-Block
CBR	Case Based Reasoning
CCS	Communications and Control Segment
CGI	Common Gateway Interface
COTS	Commercial Off-The-Shelf
CPU	Central Processing Unit
DB	Database
DNS	Domain Name Services
DT&T	Development, Test and Training
GUI	Graphical User Interface
HP	Hewlett-Packard
HTML	HyperText Markup Language
I/O	Input/Output
IP	Internet Protocol
IRM	Internetwork Response Manager
ISO	International Standards Organizations
IT	Information Technology
IT/O	IT Operations
LAN	Local Area Network
MIB	Management Information Base
NASA	National Aeronautics and Space Administration
NASCOM	NASA Communications
NCC	Network Control Center

NCCDS	Network Control Center Data Systems
NFS	Network File System
NIS	Network Information Systems
NNM	Network Node Manager
NPG	Network Protocol Gateway
NSM	Network and Systems Management
OpC	OpenView Operations Center
OSI	Open Systems Interconnect
OV	OpenView
PDF	Portable Document Format
RDBMS	Relational Database Management System
RMA	Reliability-Maintainability-Availability
RMON	Remote Monitoring
SAS	Service Accounting Segment
SDS	System Design Specification
SEWP	Scientific and Engineering Workstation Procurement
SNMP	Simple Network Management Protocol
SPSR	Service Planning Segment Replacement
SQL	Structured Query Language
SRD	System Requirements Document
SRIS	System Resources and Infrastructure Segment
STDN	Spaceflight Tracking and Data Network
TCP/IP	Transmission Control Protocol/Internet Protocol
TDRS	Tracking and Data Relay Satellite
TFTP	Trivial File Transfer Protocol
TLAS	TDRS Look Angle System
WAN	Wide Area Network
WWW	World-Wide Web
YP	Yellow Pages